communicate pu2(I,C) together with her/his application, or other form of first contact through T. As pu2(I,C) is the public part of a public encryption scheme, there is very limited risk in T knowing that key. For improved security, pu2(I,C) can be encrypted using pu1(I) before being communicated to I through T. --

---

IN THE CLAIMS:

Please amend the claims as follows.

---

1. (Amended) A method of conducting business electronically between a first party and a second party, comprising:

providing an intermediary relationship with a third party who knows an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first and second parties; and

conducting the electronic business transaction between said first and second parties through the third party such that said identity of said first party is kept from the second party,

wherein said second party is provided with information identifying said first party only as a transactional party in said electronic business transaction.

2. (Amended) A method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer, to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer; and

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity party,

wherein said business entity is provided with information identifying said customer only

as a transactional party in said electronic business transaction.

6. (Amended) The method according to claim 5, wherein said portable device P(C) generates numbers S(C,n), where n is an integer belonging to a set {1, 2, . . . , N}, and wherein for at least one of a new business unit and another partner of the customer, a new number n is chosen for all further transactions between the customer and said at least one of said new business unit and said another partner.

7. (Amended) The method according to claim 2, wherein the business entity chooses a set of verifiers Vj, j = 1, 2, . . .N, ,

wherein said verifiers are each equipped to verify portable devices, and are connectable to a network so as to output information to a third party T using privacy protection.

8. (Amended) The method according to claim 2, wherein said establishing an intermediary relationship includes sending by the customer to the third party an application to register with said business entity and software to encrypt the application using a public key pu1(I) included in a public signature scheme (Pr1(I),pu1(I)) of the business entity,

said software further allowing the customer to compute a public signature scheme (Pr2(I,C),pu2(I,C)), said application being provided over a network connected to said business entity.

15. (Amended) The method according to claim 2, wherein, with a relationship between the customer and the business entity previously established, the business entity interacts with the customer identified as a counterpart.

24. (Amended) A method of selecting a purveyor of goods or services in a confidential manner over a network, comprising:

sending, by a customer, an application to a third party along with software which allows encrypting the application using a public key pu1(I),

wherein said application is taken electronically from a business entity,

wherein a public signature scheme of said business entity is (Pr1(I),pu1(I)), said software

allowing the customer to compute a public signature scheme (Pr2(I,C),pu2(I,C)), and

wherein said business entity is provided with information identifying said customer only as a transactional party in said electronic business transaction.

---

34. (Amended) A system for conducting business electronically between a first party and a second party, comprising:

means for providing to a third party an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first party and second party; and

means for conducting the electronic business transaction between said first party and second party through the third party such that said identity of said first party is kept from the second party,

wherein said second party is provided with information identifying said first party only as a transactional party in said electronic business transaction.

35. (Amended) A signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for conducting business electronically between a first party and a second party, said method comprising:

providing to a third party an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first and second parties; and

conducting the electronic business transaction between said first and second parties through the third party such that said identity of said first party is kept from the second party,

wherein said second party is provided with information identifying said first party only as a transactional party in said electronic business transaction.

36. (Amended) A system for performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer to a business entity requiring said private data, said system comprising:

means for establishing an intermediary relationship with a third party between the candidate customer and the business entity;

a proprietary item provided to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer; and

means for performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity party,

wherein said business entity is provided with information identifying said candidate customer only as a transactional party in said electronic commerce.

37. (Amended) A signal-bearing medium tangibly embodying a program of machine- readable instructions executable by a digital processing apparatus to perform a method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer; and

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity,

wherein said business entity is provided with information identifying said customer only as a transactional party in said electronic commerce.

Please add the following new claims:

-- 38. A method of conducting business electronically between a first party and a second party, comprising:

providing an intermediary relationship with a third party who knows an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first party and the second party; and

conducting the electronic business transaction between said first party and said second party through the third party such that said identity of said first party is kept from the second party, but second party can obtain confidential data about first party that do not compromise the identity of said first party.

39. A method of conducting business electronically between a first party and a second party, comprising:

providing an intermediary relationship with a third party who knows an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first and second parties, said third party enabling communications between the first and second party and having access to the identity but not to the content or the nature of the transaction; and

conducting the electronic business transaction between said first and second parties so that the identity of said first party is not available to the second party,

wherein said second party receives confidential data about said first party unrelated to the identity of said first party.

40. The method of claim 39 wherein said first party authorizes said second party to receive confidential data about said first party.

41. A method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer, to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing an identity of said customer; and

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that the identity of said customer is unknown to said business entity,

wherein said third party can recognize, without having access to an identity, each customer to

conduct business over an extended period of time and in repeated interactions, and accumulate all data needed to service the customer, to conglomerate such data to provide a customer history or subject the data to data mining technologies.

42. The method according to claim 41, wherein a proprietary item is designed so that it cannot have more than one legitimate owner.

43. The method according to claim 41, wherein the relationship between the customer and the third party remains fixed for all further engagements with said business entity.

44. The method according to claim 41, wherein said proprietary item is provided to said first party by a fourth party.

45. The method according to claim 41, wherein a fourth party delivers to the customer a portable device P(C) which carries biometrics of the customer such that the customer can be identified as a legitimate owner of the portable device P(C) without revealing the identity of said customer.

46. The method according to claim 44, wherein said fourth party delivers to the customer a portable device P(C) which carries biometrics of the customer such that the customer can be identified as a legitimate owner of the portable device P(C) without revealing the identity of said customer. –